LUMU

IT'S TIME TO EVOLVE SECURITY TESTING

By: Fernando Cuervo

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The scientific method powered by the function of testing has enabled humans to live life as we know it today. When testing is performed with discipline, it has the power of perfecting a practice that can turn into multi-billion-dollar industries, like the commercial airline industry. Cybersecurity has still some lengths to go to evolve its testing mechanisms to make them optimal. In this paper, we discuss:

- Lessons from history perfecting the art of testing.
- Successful industries whose success is predicated on their successful testing disciplines.
- Cybersecurity's need to evolve its testing practice, as well as why current tools fall short of expectations.
- Why continuous compromise assessments are an overlooked yet critical element of cyber defense strategies.

THE GENESIS OF TESTING

Our ability to form a question that can later become a hypothesis has been an important enabler of human evolution. Parting from a moment of curiosity, humans long to understand what occurs when certain conditions are met. As such, simple and complex theories have been tested repeatedly throughout history, becoming the beginning of the scientific method as we know it today.

Rome was not built in a day, and neither are the methodologies used to test hypotheses.This has taken us several hundreds of years to get to where we are today. After a rather muted period in scientific advancement during the Dark Ages and Renaissance periods, the world experienced a time of incredible discoveries. Many european scholars became exposed: Aristotle, the greatest thinker of psychology, politics and ethics, prompted the well-known ***Dialogue Concerning the Two Chief World Systems***. Ptolemy, astronomer and geographer known for being the first to consider the Earth as the center of the universe; Euclid, known for the way space, time and shapes are conceived. Arguably, one of the most influential personas of the period was Francis Bacon, a lawyer and philosopher who was the first to formalize the concept of a true scientific method. The outcomes of his research were heavily influenced by the great minds of Nicolaus Copernicus (1473-1543) and Galileo Galilei (1564-1642) who invented the telescope, and used it to study the sun and planets.

The accomplishments of the period were the necessary setup for a radical revolution in science. The work of Isaac Newton (1642-1727) in mathematics, integral and differential calculus, and astronomy resulted in the definition of laws of motion. Newton's work marked the beginning of a new world enabled by the proper use of modern science.The success of the scientific method was further demonstrated by the creation of the cell theory, made possible by the invention of the microscope by Antoni Van Leeuwenhoek (1632-1723). This discovery served as a milestone for science in general, as it exposed the hidden world that exists beyond the limits of human vision. As such, Matthias Jakob Schleiden (1804-1881) and Zoologist Theodor Schwann (1810-1882) concluded that both all plants and all animals are composed of cells. In 1858, Rudolf Virchow (1821-1902) expanded the work of Schleiden and Schwann by proposing that all living cells must rise from pre-existing cells.These emblematic discoveries were followed by a handful of scientists that further explained how the universe functioned, including Pasteur, Einstein or Hawking.

Curiosity is the single most important element that has moved science forward. The drive to understand what lies beyond the human eye. The most important discoveries of the world have only been possible through testing a wide array of hypothesis. As such, testing is the biggest enabler of the modern world. The luxuries of life, including electricity, transportation, manufacturing, and the Internet itself are possible by relentless testing. But, what is the process that allows us to systematically take a simple question to a viable conclusion. The most simple scientific method consists of six basic steps:

1. **Make an observation:** The majority of scientific inquiry starts with an observation that piques curiosity.
2. **Ask a question:** The purpose of the question is to narrow the focus of the inquiry, to identify the problem in specific terms.
3. **Form a Hypothesis:** Suggest a possible answer in the form of a Hypothesis. A hypothesis is stated as an "if-then" statement.
4. **Conduct an experiment:** Set up to test a specific hypothesis which must be controlled.
5. **Analyze Data:** Collect quantitative and qualitative data. On that information you can find evidence to support or reject the hypothesis.
6. **Iterate:** Do it again with the new information.

There are several real world applications of testing that go beyond academic objectives. The world's most powerful armies are a perfect example, who have made use of it in preparation for war. Military groups have continuously needed to test their strategies to simulate, evaluate, perfect their defenses, and confirm these were designed and executed effectively.

The need for testing has stood the test of time from generation to generation. However, not all testing is created equal. Testing has the power to build industries, and take them from small to dominant empires. Unfortunately, testing also has the power of sabotaging industries when it is not performed diligently.

AN EXAMPLE OF WELL DONE TESTING

Now that we have settled on the criticality of testing, it is important to understand why testing is an ongoing quest for perfection proximity. Testing will point out errors in controllable and uncontrollable variables. Instead of pursuing perfection, our duty is to reach an acceptable threshold of error. Even with these acceptable thresholds, the different elements involved may very well fail. The airline industry is a good example of how precise testing can make an industry mostly predictable, and ultimately, successful. Because the effects of mechanical or process errors can be catastrophic, this industry is heavily focused on testing. Therefore, this has made flying the safest method of transportation.

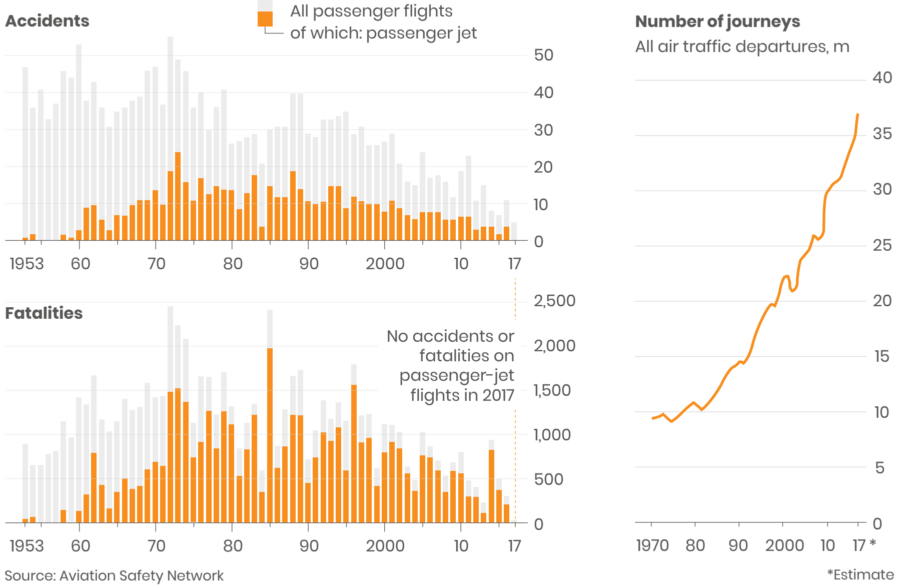
According to *The Economist*, the world saw an important decrease in the number of airplane accidents after 1972, an increase in the 80s, and a steady drop after the 90s, reaching a perfect year in 2017 with zero accidents or fatalities. Recognizing that airplane travel has become more accessible, this is an important accomplishment for the industry.

The reasons for the decrease are numbered below:

- Aviation accidents not only cost money, but also cost lives. This means, there is a sense of urgency and high pressure to solve any given problem.
- An airplane is a rather complex machine. However, the aviation industry is mostly streamlined. There are a few large vendors that manufacture aircrafts, which ensure that all the parts and procedures are standardized.
- All technology is developed with a clear purpose. After an accident, there are mandatory detailed investigations that show the root cause. This leads to the development of technology that helps ensure the same accident does not happen again. This is why the art of flying has been nearly perfected. The industry itself has pioneered an open and collaborative format to show incidents and accidents and receive support from its community.

Safer skies

Global passenger flights, number of accidents and fatalities



No accidents or fatalities on passenger-jet flights in 2017

*Estimate

Source: Aviation Safety Network

Economist.com

The entire industry is constantly trying to improve and learn from mistakes that lead to accidents. A key component to their success is their open community, where the interested parties transparently share detailed insights, accept their own errors and take actions for continuous improvement.

Aviation is the perfect example where there is a clear motivation and urgency to solve any and all problems. This is an industry that has developed the tools and methodologies to measure and continuously lower their margin of error, demonstrating the benefits of testing when done correctly. **Several other industries must learn from the airplane industry. Cybersecurity is no exception**.

THE STATE OF SECURITY TESTING

Security testing today has two big branches: penetration testing and vulnerability assessment. The first one tries to break the enterprise's defenses, and the second one shows an organization's level of exposure indirectly, demonstrating the known vulnerabilities. They focus on testing for risks outside the corporate network. How organizations organize and execute them is highly dependable on their resources. As such, these vary greatly across verticals. There are serious effects to the lack of standardized methodologies, processes, industry collaboration and transparency across the industry.

Nonetheless, there are some popular methodologies largely used by the industry:

Test Basis

- **Whitebox testing:** Full information about the target is shared with the testers.
- **Blackbox testing:** No information is shared with the testers about the target.

Test Type

- **Vulnerability identification in software:** Must give feedback to developers on coding practices.
- **Scenario to identify vulnerabilities:** The tester explore particular scenarios to find whether it leads to a vulnerability in your infrastructure.
- **Scenario to test detection and response:** The goal here is to measure the detection and response capabilities of the organization.

As an industry, we see an increased number of investments made to prevent breaches, yet we see an increased number of breaches. For a detailed review of the contributing factors to this global crisis please see **"The Need for a Breakthrough in Cybersecurity".**

WHY TRADITIONAL SECURITY TESTING IS NEEDED, BUT HARDLY ENOUGH

Penetration testing and vulnerability assessment's primary goal was to test networks, which is only part of the problem. Alone, they are insufficient, being preventive techniques. Prevention is rendered useless once compromise takes place. These tools have fallen short of expectations for the following reasons:

1. **False Hypothesis:** As we saw testing a hypothesis is the foundation of scientific method, but it is important to select the correct hypothesis to test. The hypothesis of cybersecurity in general is to test defenses assuming that we are secure, but what happens if the adversary is already inside?
2. **Incomplete:** Traditional security testing is incomplete by nature because only tests defenses and finds vulnerabilities (outside), neglecting the true state of compromise (inside).
3. **Limited View:** Traditional security testing was designed to show an image of vulnerabilities of critical assets in a specific date, but systems, configurations and threats change on a daily basis.
4. **Relies on the weakest link:** The industry assumes that the attacker gets inside the networks exploiting vulnerabilities but the truth is that it is easy to send an email to compromise an organization. We rely on people to not be in a compromising position which is unrealistic.

The purpose of penetration testing is to simulate whether an attacker can pass an organization's defenses. These tests are not conclusive.Often, pentesters have different abilities when compared to the attacker as well as less time to perform each test. In the case of vulnerability assessments, the single purpose is to measure the exposure of a company. These tests are performed based on hypothetical scenarios of potential exploitation vectors from the attacker. This means, organizations can learn about the potential of attacks instead of confirmed attacks.

An additional shortcoming of pentests is their focus exclusively on the critical assets. As an industry, we have a misconception that all attacks occur on servers and databases. The truth is that most attacks start with malicious email targeting the employees, meant to compromise a device and move laterally until higher value assets are found. Lastly, organizations often still rely on legacy systems difficult or impossible to upgrade. Such systems may be exposing them to a wide range of vulnerabilities, that penetration testing may detect. However, it may not be possible to take action due to the legacy nature of the systems.

The reasons exposed above are not meant to discourage penetration testing and vulnerability assessments. However, the industry as a whole has set unrealistic expectations on these tools, that exceed what they were designed to do. They are certainly not where testing should end. In fact, the way the industry executes testing is useful, but hardly enough.

The greatest evidence that we are missing a part on our security strategy is that there are breaches making headlines weekly, even in companies that devote a lot of resources and are compliant to pentesting and vulnerability assessment regulatory requirements.

THE EVOLUTION OF SECURITY TESTING

Testing has a critical role in the evolution of today's digitally-driven, ever-connected world. The life humans carry out is only possible because of the perfection of the testing discipline. Everything that humans see, touch and experience, requires an enormous amount of testing before it becomes a reality. Because the more one improves the testing practice, the better the outcome, testing has the power of building up an entire industry. Unfortunately, the opposite is also true.

Cybersecurity is yet to perfect the art of testing for the greater good of the industry. We have already analyzed why testing in cyber is severely flawed but it is worth pondering on the fact that organizations rarely find vulnerabilities that they are not purposely looking for and determined to find. It is likely that compromises are not found because they are not actively being looked for. This fact certainly merits the question: **Why organizations are not diligently and systematically determined to identify compromises?**

Recent incidents demonstrate that adversaries have remained inside of enterprise networks for long periods of time, going absolutely undetected, even after the execution of multiple pentests and vulnerability assessments.

Breach	Dwell time
Citrix	10 years
Marriott	4 years
Yahoo	Several Breaches. Months.
Equifax	6 months

The most overlooked component of cybersecurity testing is the hypothesis that networks are compromised. The focus is placed on the erroneous assumption that organizations are secured, and no compromise exists. There is a famous quote by Steve Denn that depicts the described situation: *"One can never make the same mistake twice, because the second time, it is not a mistake, it is a choice."* As an industry, the mistaken assumption should no longer be considered an error, but instead an action that is taken deliberately.

As we adjust the standard scientific method to fit the needs of the cybersecurity industry, the steps below must be followed:

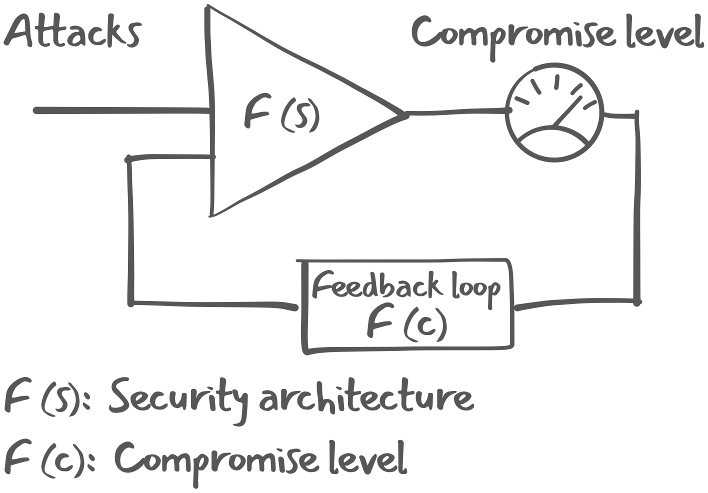
1. **Make an observation:** The cybersecurity industry is underperforming. Data breaches continue to grow in scale and sophistication, despite investment surges.
2. **Ask a question:** Why do breaches continue to happen?
3. **Form a Hypothesis:** If we evolve the security testing methods then the breaches will decrease.
4. **Conduct an experiment:** Analyze network data to find compromises. Check if this information provides additional value when compared to traditional security testing.
5. **Analyze Data:** Analyze how those findings improve or not an organization's stance against risk and whether it is improving its cyber-resilience.
6. **Iterate:** Develop a "rinse and repeat" culture. Repeat the process with additional information.

It is imperative to urge organizations to assume their networks are compromised, and work tirelessly to prove otherwise. **This is the most critical hypothesis that security practitioners must be continuously testing**. The most critical step is to admit that organizations must challenge the status quo and evolve their thinking if different results are desired.

Here are some points to start this evolution:

1. **Mindset change.** There is a need to internalize the assumption of being compromised and focus on proving that it is not the case. Keep in mind that traditional security testing is needed but not enough. If organizations want to be cyber-resilient, **measuring compromise** is not negotiable.
2. **Unlock the value of the organization's own data.** Organizations are sitting on a gold mine: their own network data. Pro Tip: DNS queries are possibly the most valuable information for compromise detection and only a few companies are using it.
3. **Engage in continuous compromise assessment.** Once the data is unlocked, the visibility and intelligence can be extremely valuable. A continuous compromise assessment program can ensure that compromise is detected dynamically and in real-time. Measure effectiveness. Start with a baseline and take deliberate actions to eliminate the compromise, and increase your cyber-resilience.

The single purpose of most of the cyber defense strategies is to avoid being compromised. Yet, this is useless if a compromise happens, and, the function of detecting and measuring compromise is absolutely neglected. Continuous compromise detection has become a necessity. Organizations that can unlock what hides under their own data will become empowered to perfect their defense strategies. For this reason, the feedback loop between defenses implemented and compromise detection must be closed. The diagram below explains it in detail:



© Lumu Technologies.

Compromise detection complements existing testing and vulnerability tools, and helps companies evolve and perfect their own testing practice. Today, the cybersecurity industry faces a solid opportunity: to arm organizations with the right knowledge on compromised levels through the implementation of tried and true testing methodologies.

CONCLUSIONS

The world as we know it is largely enabled by the testing discipline. None of the luxuries of modern life are exempt from this phenomenon. Deliberately designed testing practices produce transformational results. In cybersecurity, we have the duty to design the testing practice the space needs and deserves, while being accountable for the results. As we stand today, there is significant evidence that:

- Traditional security testing is needed but not enough.
- Organizations need to unlock the value of their own data, as it is the most overlooked gold mine.
- Measuring compromise is key for fine tuning cyberdefense. Closing the feedback loop is a key step in the process.

We must improve our industry's security testing and look beyond the reduction of financial losses. Cybercriminals have the power to damage enterprises but also put nations at risk. The risk can only be contained if we actively look for compromise, and make this a foundational component of our security testing frameworks and strategies. This fundamental shift is in our hands to execute, and there is no time to waste.

REFERENCES

[1] "Aristotle | Biography, Contributions, & Facts," Encyclopedia Britannica. [Online]. Available: https://www.britannica.com/biography/Aristotle. [Accessed: 22-Oct-2019].

[2] "Aviation Safety Digest." [Online]. Available: https://www.atsb.gov.au/aviation/aviation-safety-digest/. [Accessed: 23-Oct-2019].

[3] "Cell Theory | HowStuffWorks." [Online]. Available: https://science.howstuffworks.com/innovation/scientific-experiments/scientific-method4.htm. [Accessed: 22-Oct-2019].

[4] "Citrix Systems Breached 'for 10 Years by Iran,' Claims Unknown Infosec Firm," Security Boulevard, 12-Mar-2019. [Online]. Available: https://securityboulevard.com/2019/03/citrix-systems-breached-for-10-years-by-iran-claims-unknown-infosec-firm/. [Accessed: 23-Oct-2019].

[5] "Cost of a Data Breach Study | IBM." [Online]. Available: https://www.ibm.com/security/data-breach?cm_mmc=Search_Google-_-Security_Optimize+the+Security+Program-_-WW_NA-_-%2Bdata%20%2Bbreach%20%2Bcost_b&cm_mmca1=000000NJ&cm_mmca2=10000253&cm_mmca7=1003659&cm_mmca8=aud-322244832184:kwd-295901325779&cm_mmca9=CjwKCAjw9L_tBRBXEiwAOWVVCQ4iRVM5ekbyoLcoFKzP0YrYXYuHyZ83Y4-eBC_7QVj7Wd85woO7shoCP9AQAvD_BwE&cm_mmca10=376283678765&cm_mmca11=b&gclid=CjwKCAjw9L_tBRBXEiwAOWVVCQ4iRVM5ekbyoLcoFKzP0YrYXYuHyZ83Y4-eBC_7QVj7Wd85woO7shoCP9AQAvD_BwE&gclsrc=aw.ds. [Accessed: 23-Oct-2019].

[6] "Full text of 'Galilei, Galileo - Dialogue Concerning the two Chief World Systems.'" [Online]. Available: https://archive.org/stream/GalileiGalileoDialogueConcerningTheTwoChiefWorldSystemsEN155P./Galilei%2C+Galileo+-+Dialogue+Concerning+the+two+Chief+World+Systems+%28EN%2C+155+p.%29_djvu.txt. [Accessed: 22-Oct-2019].

[7] "Verizon Data Breach Investigations Report - 2018." [Online]. Available: https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-2018. [Accessed: 23-Oct-2019].

Illuminating threats
and adversaries

www.lumu.io

Lumu Technologies Inc. | 8350 NW 52nd Terrace Suite 301, Miami, FL 33166 | info@lumu.io | +1 (877) 909-5868